HBMA Billing Company Educational Resource:

Business Associate Agreement with Sample HITECH Act Provisions.

As a part of its ongoing commitment to support the compliance activities of its Members, the HBMA has presented a series of webinars and other educational efforts over the past year designed to make its Members aware of the impact of the HITECH Act on third party billing companies, particularly in their capacity as a HIPAA Business Associate of the physicians and other health care providers that third party billing companies serve. **[*Members can access materials from those presentations at _____].***

Before the HITECH Act, Business Associate Agreements were a relatively straight-forward contractual statement of specific requirements set forth in the HIPAA Privacy Rule, requirements. In general, these requirements were uniformly applicable across billing companies and even across industries. The HITECH Act changed all that. Among other things, the HITECH Act:

- Makes Business Associates subject to direct enforcement for HIPAA violations, just as their client Covered Entities are;

- Imposes direct reporting obligations on Business Associates as to breaches of the security of Protected Health Information created by the Business Associate or held under the Business Associate's control;

- Requires Business Associates to comply with specific elements of the HIPAA Security Standards, including having specific types of physical, administrative and technical safeguards in place for Protected Health Information in electronic form together with written policies and procedures in place that implement those safeguards;

- Provides individuals with a number of new rights as to their Protected Health Information. These new rights result in new obligations for Covered Entities and Business Associates. Of particular concern for billing companies are the HITECH Act provisions which:

    - In certain circumstances, require billing companies to provide HIPAA accounting information for disclosures by the Business Associate for payment purposes for a rolling three year period; and

    - Permit individuals to require that information about services paid for entirely out-of-pocket not be disclosed to Health Plans for payment purposes unless the disclosure is requried by law.

A general overview of the HITECH Act changes to HIPAA from February 2009, titled "Health Care Information, Privacy and Security Bulletin" is provided with this Sample Business Associate Agreement. It is recommended that Members review this document before working through the following Sample Business

Associate Agreement.

The HBMA originally published a sample Billing Company Business Associate Agreement in 2003, along with the HBMA model Billing Services Agreement, for use in connection with HBMA educational presentations[1]. The Sample Business Associate Agreement which follows is a version of that Agreement which has been updated to reflect the 2005 "Security Incident" provision required by the HIPAA Security Standards and to provide illustrative provisions reflecting the requirements of the HITECH Act that are generally applicable to billing companies. Not all HITECH provisions are included in the Sample Business Associate Agreement[2]. In order to help Members focus on the HITECH Act illustrative language, a red line is also provided, showing the changes from the original version.

In the post-HITECH Act legal environment, many aspects of Business Associate Agreements will be subject to negotiation, reflecting the significant new responsibilities of Business Associates and the complexity of many of the requirements. Members must understand that there is no longer any such thing as a "standard" Business Associate Agreement, applicable to any third party billing company. Members should work with their individual health care consultants and legal counsel to ensure that their Business Associate Agreement not only meets the requirements of the HITECH Act but also is consistent with the company's Billing Services Agreement, technological capabilities and general philosophy of legal compliance. This HBMA sample Business Associate Agreement contains sample clauses that are designed to illustrate possible approaches to this task.

In order to help guide Members and their advisors through some of the decisions that will determine the specific HITECH Act provisions appropriate to the Member, some general comments are provided below:

1. To amend or not to amend: Two key provisions of the HITECH Act, "Application of Privacy Provisions and Penalties to Business Associates of Covered Entities" and a parallel provision referring to the HIPAA Security Standards, each state that the additional requirements of the HITECH Act that relate to privacy or security and that are made applicable with respect to Covered Entities shall also be applicable to Business Associates of the Covered Entity "*and shall be incorporated into the business associate agreement between the business associate and the covered entity".* This phrasing has given rise to an ongoing debate in the legal and consulting community as to whether the HITECH

[1] Like the Billing Services Agreement, this Business Associate Agreement is provided for educational and illustrative purposes. It does not constitute legal or consulting advice by the HBMA or its authors / presenters. Members must consult with their own legal counsel and health care consultants about terms and provisions that are appropriate for the Member's individual situation.

[2] For example, to the extent a billing company provides other services, such as provision of an EMR / EHR access to practice management software hosted by the billing company, the provisions of this sample Billing Company Agreement may not be complete or appropriate.

Act requires Covered Entities and their Business Associates to amend their written business associate agreement or whether some or all of the HITECH Act provisions apply automatically, by operation of the law, without the need for amendment by the parties. It is expected that the Secretary of Health and Human Services will provide guidance on this issue, but with many of the HITECH Act provisions becoming effective on February 17th, 2010, The attached Sample Business Associate Agreement takes the approach of amending the Business Associate Agreement, with as much flexibility built into the HITECH Act provisions as possible, so that it can adapt to future clarifications with minimum further amendments. Ultimately, the decision to amend or not amend has potential legal consequences and risks that each Billing Company must assess with its legal counsel.

2. Security Incident. Business Associates have, since 2005, been requried to report a "Security Incident" to the Covered Entity. The Security Standard's definition of a Security Incident appears in the sample Business Associate Agreement at Section 1 (l) of the Definitions, word-for-word. The HITECH Act concern is that there is no clear line between a Security Incident and a Breach involving Unsecured Electronic Protected Health Information, a significant provision of the HITECH Act which is discussed below. The issue is that a Security Incident is defined to include attempts to interfere with an information system, requiring reporting even if there is no actual interference or improper access and, by extension, no Breach. Many information systems experience numerous attempts to access the system improperly every day and the burden of reporting unsuccessful attempts could be significant and reports of unsuccessful attempts may not be of interest to the Covered Entity. Some Business Associates attempt to "carve out" unsuccessful attempts from their reporting obligation, despite the wording of the definition of Security Incident, by excluding the obligation to report a Security Incident which is unsuccessful, if the unsuccessful attempt does not reasonably pose a risk of disclosure, modification, or destruction of information or interference with system operations. The thought is that simply being "pinged" by a potential hacker does not need to be reported, although an attack that was successfully defeated by the information system's security before any actual penetration into the system's servers or data base might be reportable. Billing companies are cautioned to consult with legal counsel before taking any such position as to unsuccessful Security Incidents, given the regulatory definition of a Security Incident.

3. Compliance with the HIPAA Security Standards. Pre-HITECH Act, the HIPAA Privacy Rule simply required a Covered Entity to obtain an assurance from each Business Associate that appropriate safeguards would be employed to protect the Covered Entity's Protected Health Information in the hands of the Business Associate. This language appears in the Sample Business Associate Agreement at Section 2 (b) and continues to apply to Protected Health Information in paper form. However, under the HITECH Act, if the Business Associate maintains Protected Health Information in electronic form (so-called "ePHI"), the Business Associate must, in the same manner as a Covered Entity, comply with the detailed requirements of the HIPAA Security Standards by selecting and applying qualifying Physical, Administrative and Electronic security

measures and by having written Policies and Procedures implementing those measures. This is a formal process requiring, among other things, a documented Risk Assessment of the Business Associate's systems. The Security Standards establish elements that are "Requried", such as the Risk Assessment, and elements that are "Addressable" such as encryption and of the Business Associate's decisions as to how to comply with "Addressable" requirements, in particular, should be documented. The HITECH Act obligations are also set out in Section 2 (b) of the Sample Business Associate Agreement. This subject of compliance with the Security Standards has been discussed in prior HBMA webinars. A link to the text of the Security Standards and an outline of the Requried and Addressable elements compliance is available on the HBMA Website through the HITECH hotlink.

4. Breach of Security of Unsecured Protected Health Information. One of the most significant provisions of the HITECH Act imposes on Business Associates and Covered Entities the obligation to report to individuals, and in some cases, to the Secretary, a Breach of the Security of Unsecured Protected Health Information, whether that information is in electronic, paper or even oral form. A Breach is defined in Section 1 (b) of the Definitions, tracking the language of the HITECH Act. The steps that must be taken to render Protected Health Information "Secure", and therefore not subject to Breach notification requirements, were published by the Secretary in the August 24, 2009 Federal Register, beginning at page 42740, and are available on the HBMA website through the HITECH Act. These standards, basically encryption under an approved methodology for ePHI and destruction for ePHI or paper PHI, require strict compliance for Protected Health Information to be deemed Secure. The Breach notification requirements themselves require careful drafting and, in some cases, negotiation with clients to protect the Billing Company from liability and undue burden while assuring the client that the Billing Company will cooperate as requried by the HITECH Act. An Interim Final Rule made the Breach Notification provisions effective on September 23, 2009, although federal imposition of penalties for failure to provide individuals with notice was suspended until February 23, 2010 in order to allow Covered Entities and Business Associates time to put appropriate procedures in place**.** The Interim Final Rule can be accessed on the HBMA website through the HITECH hotlink. Significant clarifications are possible when the Final Breach Notification Rule is published, although no date has been established for that publication.

Section 2 (c) (1), (2) and (3) of the Sample Business Associate Agreement contain provisions that attempt to anticipate and deal with possible issues that can arise between a Billing Company and its Clients in this context. Billing Companies should work with their health care consultants and legal counsel to determine if this approach is appropriate for the Billing Company and will be acceptable to its Clients.

5. Accounting for Treatment, Payment and Health Care Operations Disclosures. Section 2 (i) of the Sample Business Associate Agreement contains a provision that deals with one of the most potentially burdensome requirements of the HITECH Act for Billing Companies: the obligation to provide information

requried for a HIPAA accounting for Treatment, Payment and Health Care Operations disclosures by the Billing Company. Since this provision is unclear on the face of the HITECH Act and specifically requires implementing regulations before it becomes effective, a Billing Company and its legal counsel may decide to omit such a provision at this time, and seek to amend the Business Associate Agreement when those regulations are published. The language in the Sample Business Associate Agreement represents an approach that deals with the issue in a flexible manner that may obviate the need for such an amendment.

6. Prohibition on Direct or Indirect Remuneration in Exchange for Protected Health Information. Section 2 (k) of the Sample Business Associate Agreement contains another HITECH Act provision that is not well articulated in the Act and requires implementing regulations. Billing Companies and their legal counsel could decide to defer dealing with this issue, as discussed in the preceding paragraph. Section 2 (k) represents an approach to dealing with the requirements in a general way that may remove the need for subsequent amendments to the Business Associate Agreement.

7. Restriction on Reporting Self-Pay Services to Health Plans. One of the HITECH Act provisions with the most troublesome operational implications for third party billing companies is the right of an individual to requried a Covered Entity to refrain from disclosing services that are paid for entirely out-of-pocket by the individual to a Health Plan for payment or health care operations purposes, unless such disclosure is "required by law". This provision of the HITECH Act is fraught with legal and operational issues that need to be reviewed carefully by Billing Companies and their legal counsel.

The general approach taken in Section 4 (b) of the Sample Business Associate Agreement requires advance notice of such a restriction, sufficient to allow the Billing Company to stop the process of filing of a claim for a qualifying self-pay service. The period of notice will depend on the technological capabilities of the individual Billing Company. The Sample Business Associate provision also puts the burden on the Medical Practice to make required legal determinations as to whether disclosure is requried by law and contains contractual protections for the Billing Company acting in reliance on its client's instructions.

8. Amendment. Section 7 (c) of the Sample Business Associate Agreement contains an example of a flexible Amendment clause permitting either the Billing Company or the Medical Practice to seek mutually agreed amendments to the Business Associate Agreement, if amendments are necessary to deal with changes to or clarifications of the HITECH Act. It is one of the many possible approaches to this issue that a Billing Company and its legal counsel should consider, particularly as to the right of either the Billing Company or the Medical Practice to terminate the Billing Services Agreement if the parties are unable to agree on appropriate amendments.

HBMA SAMPLE BILLING COMPANY BUSINESS ASSOCIATE AGREEMENT

This Business Associate Agreement ("Agreement") is entered into between _____ ("Medical Practice") _____ ("Billing Company") and is effective as set forth in Section 6 (a) below.

RECITALS

A. Business Associate provides certain billing and collection services to Covered Entity pursuant to a written Service Agreement.

B. Under the Service Agreement, Medical Practice discloses certain information ("Information") to Billing Company so that Billing Company can perform on Medical Practice's behalf certain functions or activities relating to treatment, payment and / or health care operations of Medical Practice, some of which information constitutes Protected Health Information ("PHI") as defined under the Health Insurance Portability and Accountability Act of 1996, Public Law 104-191 ("HIPAA").

C. The purpose of this Agreement is to satisfy certain standards and requirements of HIPAA and the HIPAA Regulations, including, but not limited to, Title 45, Section 164.504(e) of the Code of Federal Regulations ("CFR"), as the same may be amended from time to time.

In consideration of the mutual promises below and the exchange of information pursuant to this Agreement, the parties agree as follows:

1. **Definitions.** Unless otherwise defined in this Agreement, capitalized terms have the meanings ascribed to them under HIPAA, the HIPAA Privacy Rule and Security Standards, as amended by the HITECH Act:

   (a) *Billing Company.* "Billing Company" shall mean _____, functioning as a Business Associate of Medical Practice pursuant to the Service Agreement and as such term is defined under the HIPAA Regulations, including, but not limited to 45 CFR Section 160.103.

   (b) *Breach*. "Breach" means the unauthorized acquisition, access, use, or disclosure of Protected Health Information which compromises the security or privacy of such information, except where an unauthorized person to whom such information is disclosed would not reasonably have been able to retain such information. The term "Breach" does not include acquisition, access, or use made in good faith and within the course and scope of the employment or other professional relationship of such employee or individual with Billing Company if such information is not

further acquired, accessed, used, or disclosed by any person; or any inadvertent disclosure from an individual who is otherwise authorized to access Protected Health Information at a facility operated by Billing Company to another similarly situated individual at same facility if such information received as a result of such disclosure is not further acquired, accessed, used, or disclosed without authorization by any person or other circumstances specified in Regulations or Guidance issued by the Secretary.

(c) *Data Aggregation Services*. Date Aggregation Services means the combining by Billing Company of the Protected Health Information of Medical Practice with Protected Health Information received by Billing Company in its capacity as a Billing Company of another Medical Practice to permit data analyses that relate to the health care operations of Medical Practice or other Covered Entities.

(d) *Medical Practice.* "Medical Practice" shall mean _____, functioning as a Covered Entity under HIPAA as described in the Service Agreement and as such term under HIPAA and the HIPAA Regulations, including, but not limited to, 45 CFR Section 160.103.

(e) *Designated Record Set.* "Designated Record Set" shall mean a group of records maintained by or for Medical Practice that are (i) the medical records and billing records about individuals maintained by or for Medical Practice; (ii) the enrollment, payment, claims adjudication, and case or medical management record systems maintained by or for a health plan; or (iii) used, in whole or in part, by or for the Medical Practice to make decisions about individuals. For purposes of this definition, record means any item, collection, or grouping of information that includes protected health information and is maintained, collected, used, or disseminated by or for Medical Practice.

(f) *Guidance.* "Guidance" shall mean official guidance of the Secretary as specified in the HITECH Act and any other official guidance or interpretation of HIPAA by a federal governmental agency with jurisdiction.

(g) *HITECH Act*. "HITECH Act" shall mean the Health Information Technology for Economic and Clinical Health Act, enacted as Title XIII, Subtitle D of the American Recovery and Reinvestment Act or 2009, and implementing Regulations and Guidance.

(h) *Individual*. "Individual" shall have the same meaning as the term "individual" in 45 CRF 164.501 and shall include a person who qualifies as a personal representative in accordance with 45 CFR 164.502(g).

(i) *Privacy Rule*. "Privacy Rule" shall mean the Standards for Privacy of Individually Identifiable Health Information at 45 CFR part 160 and part 164, subparts A and E, as amended by the HITECH Act.

(j) *Protected Health Information or PHI and ePHI* "Protected Health Information" and "PHI" shall have the same meaning as the term "protected health information" in 45 CFR 164.501. References to PHI shall be deemed to include references to PHI in electronic form held by Billing Company ("ePHI") unless stated otherwise. Billing Company's obligations under this Agreement apply only to Protected Health Information created or received by Billing Company from or on behalf of Medical Practice, and the term Protected Health Information refers only to Protected Health Information created or received by Billing Company from or on behalf of Medical Practice under the Service Agreement.

(k) *Required By Law*. "Required By Law" means a mandate contained in law that compels Billing Company or Medical Practice to make a use or disclosure of Protected Health Information and that is enforceable in a court of law. Required by Law includes, but is not limited to, court orders and court-ordered warrants; subpoenas or summons issued by a court, grand jury, a governmental or tribal inspector general, or an administrative body authorized to require the production of information; a civil or an authorized investigative demand; Medicare conditions of participation with respect to health care providers participating in the program; and statutes or regulations that require the production of information, including statutes or regulations that require such information if payment is sought under a government program providing public benefits.

(l) *Security Incident.* "Security Incident" means the attempted or successful unauthorized access, use, disclosure, modification, or destruction of information or interference with system operations in an information system.

(m) *Security Standards.* "Security Standards" shall mean the Security Standards at 45 CFR parts 160, 162 and 164, as may be amended or supplemented during the term of this Agreement and all applicable Guidance.

(n) *Service Agreement*. "Service Agreement" shall mean the agreement or agreements between Medical Practice and Billing Company under which Billing Company performs third party billing or other specified functions or activities on behalf of Medical Practice which involve the PHI of Medical Practice. In the event there are multiple Service Agreements, this Agreement shall be interpreted as applying separately to each.

(o) *Secretary*. "Secretary" shall mean the Secretary of the Department of Health and Human Services or her designee.

(p) "*Unsecured Protected Health Information*" Unsecured Protected Health Information means Protected Health Information that is not secured through the use of a technology or methodology specified by the Secretary in published Regulations or Guidance.

2. Obligations and Activities of Billing Company as to Protected Health Information.

(a) Billing Company agrees to not use or further disclose Protected Health Information other than as permitted or required by the Service Agreement, this Agreement or as required by law.

(b) Billing Company agrees to use appropriate safeguards to prevent use or disclosure of the Protected Health Information other than as provided for by the Service Agreement and /or this Agreement. As to ePHI, Billing Company will comply with the applicable provisions of the Security Standards, by providing Administrative, Physical, and Technical Safeguards for all ePHI and by developing Policies and Procedures implementing those Safeguards.

(c) (1) Billing Company agrees to report to Medical Practice any use or disclosure of the Protected Health Information not provided for by the Service Agreement and/or this Agreement. Without limiting the foregoing, Billing Company agrees to report to Medical Practice any Breach of Protected Health Information accessed, maintained, retained, modified, stored, destroyed or otherwise held or used in Unsecured form by Billing Company. Billing Company will provide written notice of any such Breach to Medical Practice in the manner and to the recipient designated in the Service Agreement, unless the parties agree in writing in advance on another method or recipient of such notice, within ____ (__) business days of the first day the Breach is known, or reasonably should have been known, to the Billing Company, including for this purpose known to any employee, officer, or other agent of the Billing Company (other than the individual committing the Breach) ("Breach Notice"). The Breach Notice will include the identification of each individual whose Unsecured Protected Health Information was subject to the Breach, the nature of the PHI that was subject to the Breach and the circumstances of the Breach, to the extent known to Billing Company as of the date of the Breach Notice. Billing Company will take reasonable steps to mitigate the effects on the Breach, coordinating such efforts with the Medical Practice. Billing Company will diligently pursue investigation of the Breach and notify Medical Practice in writing as soon as reasonably possible, but in no event later than _____ (__) business days after the date of the Breach Notice of the names of all individuals whose Unsecured PHI was subject to the Breach, of the full circumstances of the Breach and of any other

information related to the Breach Billing Company discovers, all to the extent available to Billing Company after using all reasonable efforts to investigate. Billing Company will promptly provide other information relating to the Breach as reasonably requested by Medical Practice and available to Billing Company.

(2) Unless the parties specifically agree otherwise in writing, notice to individuals or governmental agencies will be provided solely by Medical Practice, in a form and with content determined by Medical Practice, provided that (i) Medical Practice will discuss, in advance of any decision by the Medical Practice as to providing notice to individuals, the Secretary or other agencies, any harm threshhold analysis (whether under the HITECH Act or under applicable Regulations or Guidance) made by the Covered Entity as to the Breach and (ii) be given a copy of any proposed notice and a list of its intended recipients, in both cases at least _____ (__) days in advance. During that time period, and Billing Company may provide comments to Medical Practice as to accuracy and completeness of the harm threshhold analysis or the statements contained in the notice, which comments will be reasonably considered by the Medical Practice. Unless specifically provided otherwise in the Service Agreement, Billing Company will be deemed an independent contractor, and not an agent, of Medical Practice for purposes of Breach Notification. In the event that the Breach also implicates a state law requiring notification of individuals or agencies, Billing Company will have the same rights as to the notice to be given by Medical Practice specified above.

(3) In the event that Medical Practice experiences a Breach, other than a Breach solely and directly attributable to the Billing Company, by Billing Company, and requests Billing Company's assistance in analyzing or responding to the Breach, Billing Company will use reasonable efforts to comply, provided that Billing Company may charge Medical Practice reasonable amounts for time and materials provided, which will be paid promptly by Medical Practice upon receipt of a statement therefor and provided further that Medical Practice is solely responsible for all aspects of the content, timing and provision of notice to individuals and agencies.[3]

(d) Billing Company agrees to mitigate, to the extent practicable, any harmful effect that is known to Billing Company of a use or disclosure of Protected Health Information by Billing Company in violation of the requirements of this the Service Agreement and / or Agreement.

[3] Neither the HBMA nor its representatives recommend any particular level or method of calculation of a billing company's fees and charges. Such decisions are solely those of the individual billing company, based on its costs, the nature of its services, local market conditions and other factors considered relevant by the billing company. However, certain HITECH Act provisions, such as the foregoing, have the potential to cause a billing company to incur additional costs. In this educational and illustrative Sample Billing Company Business Associate Agreement, references to additional charges are included to solely alert billing companies to that possibility.

(e) Billing Company agrees to ensure that any agent, including a subcontractor, to whom it provides Protected Health Information received from, or created or received by Billing Company on behalf of Medical Practice agrees to the same restrictions and conditions that apply through this Agreement to Billing Company with respect to such information.

(f) To the extent Billing Company maintains an original Designated Record Set an behalf of Medical Practice, Billing Company agrees to provide access, at the request of Medical Practice, and in the time and manner designated by Medical Practice, to Protected Health Information in a Designated Record Set, to Medical Practice in order to meet the requirements under 45 CFR 164.524.

(g) Billing Company agrees to make any amendment(s) to Protected Health Information in a Designated Record Set maintained by Billing Company that the Medical Practice directs or agrees to pursuant to 45 CFR 164.526, at the request of Medical Practice, and in the time and manner reasonably designated by Medical Practice.

(h) Billing Company agrees to make internal practices, books, and records relating to the use and disclosure of Protected Health Information received from, or created or received by Billing Company on behalf of Medical Practice available at the request of the Medical Practice to the Secretary, in a time and manner designated by the Secretary, for purposes of the Secretary determining Medical Practice's compliance with the Privacy Rule.

(i) Billing Company agrees to document such disclosures of Protected Health Information and information related to such disclosures as would be required for Medical Practice to respond to a request by an Individual for an accounting of disclosures of Protected Health Information in accordance with 45 CFR 164.528. If Medical Practice uses or maintains an Electronic Health Record(s), as defined in the HITECH Act, Medical Practice will advise Billing Company of that fact and Billing Company and Medical Practice will meet and discuss whether Billing Company's accounting obligations are requried under the HITECH Act to include disclosures by Billing Company for purposes of Treatment, Payment and Health Care Operations ("TPO Accounting"); provided that: (i) Medical Practice will provide such notice to the Billing Company at least _____ (___) in advance of the effective date of disclosures that Billing Company is obligated to report disclosures for a TPO Accounting under this paragraph; and (ii) Billing Company may make a reasonable additional charge, on an accounting-by-accounting basis or through an upward adjustment to its fees or cost pass-throughs under the Service Agreement, reasonably calculated to cover Billing Company's additional costs to provide such a TPO accounting[4]. TPO Accounting shall be provided in accordance with Regulations promulgated by the Secretary.

[4] See footnote 3.

Unless the parties agree otherwise, in writing, in the event of an individual's request for an accounting, Business Associate will provide information it is requried to maintain pursuant to this Agreement to Medical Practice and Medical Practice will provide the accounting to the individual.

(j) Upon reasonable advance notice, Billing Company will provide individuals with access to their Protected Health Information in an electronic format and transmit such information in electronic format directly to an entity specified by the individual, to the extent the individual's PHI is Medical Practice's PHI held or controlled by Billing Company, in accordance with the HITECH Act amendments to the Privacy Rule. Billing Company may make a reasonable charge to Medical Practice or to, to the extent permitted by the HITECH Act, Regulations, or Guidance, the individual for such transmission[5].

(k) As of the date six (6) months after the Secretary issues applicable final Regulations, Billing Company will not, directly or indirectly, exchange Medical Practice's PHI or Medical Practice's Electronic Health Records for direct or indirect remuneration unless specifically provided for in the Service Agreement. In this regard, Billing Company will comply with applicable Regulations to be published by the Secretary.

3. Permitted Uses and Disclosures of Protected Health Information by Billing Company. Except as otherwise limited in the Agreement and/or this Agreement, Billing Company may use or disclose Protected Health Information to perform functions, activities, or services for, or on behalf of, Medical Practice as specified in the Service Agreement, provided that such use or disclosure would not violate the Privacy Rule if done by Medical Practice, including the following:

(a) Except as otherwise limited in this Agreement, Billing Company may disclose Protected Health Information for the proper management and administration of the Billing Company or to carry out legal responsibilities of Billing Company, provided that disclosures are required by law, or Billing Company obtains reasonable assurances from the person to whom the information is disclosed that it will remain confidential and used or further disclosed only as required by law or for the purpose for which it was disclosed to the person, and the person notifies the Billing Company of any instances of which it is aware in which the confidentiality of the information has been breached.

(b) Billing Company may use Protected Health Information to provide Data Aggregation services to Medical Practice as permitted by 45 CFR 164.504(e)(2)(i)(B) to the extent required under the Service Agreement.

(c) Billing Company may use Protected Health Information to create information that is not individually identifiable health information, as permitted by 45 CFR 164.502(d) and 164.514 ("De-identified Information"). Billing Company shall

[5] See footnote 3.

own the De-identified Information, under copyright and all other applicable laws or legal doctrines.

4. Obligations of Medical Practice to Inform Billing Company of Privacy Practices and Individual Restrictions.

(a) Medical Practice shall provide Billing Company with the notice of privacy practices that Medical Practice produces in accordance with 45 CFR 164.520, as well as any changes to such notice.

(b) Medical Practice shall notify Billing Company of any restriction on the use or disclosure of Protected Health Information that Medical Practice has agreed to in accordance with the Privacy Rule, to the extent that such restriction may affect Billing Company's use or disclosure of Protected Health Information at least ___ (___) in advance of the date upon which compliance by the Billing Company is requried. If Medical Practice agrees not to disclose an item or service paid for entirely out-of-pocket by an individual to a Health Plan for payment or health care operations purposes, unless such disclosure is requried by law ("Self-Pay Services"), the following additional conditions shall apply: (i) Medical Practice is solely responsible for determining whether there is an applicable legal requirement that requires such disclosure; (b) Billing Company may rely on Medical Practice's instructions not to disclose; and (iii) Medical Practice will indemnify and hold Billing Company harmless from costs or damages arising from such reliance. Billing Company may make a reasonable charge, on an instance-by-instance or other basis, for compliance with Medical Practice's instructions and Medical Practice will pay such charges promptly upon receipt of an invoice or statement[6]. Billing Company will use all reasonable efforts comply with all such limitations subject to timely receipt of notice from Medical Practice as specified above.

5. Permissible Requests or Disclosures

Except as specifically provided in the Service Agreement or in this Agreement, Medical Practice shall not request Billing Company to use or disclose Protected Health Information in any manner that would not be permissible under the Privacy Rule if done by Medical Practice. Without limiting the generality of the foregoing, under the Service Agreement, Medical Practice will provide, and Billing Company will request, no more than, the minimum necessary amount of Medical Practice PHI required for the performance of Billing Company's services under the Service Agreement. Billing Company and Medical Practice will comply with the Guidance on minimum necessary to be issued by the Secretary as to the Minimum Necessary as reasonably requested by Medical Practice.

[6] See footnote 3.

6. Term and Termination

(a) *Term*. This Agreement is effective as of as of _____ and replaces any prior Business Associate Agreement between the parties relating to the Service Agreement. This Agreement shall terminate when the Service Agreement terminates and all of the Protected Health Information provided by Medical Practice to Billing Company, or created or received by Billing Company on behalf of Medical Practice, is destroyed or returned to Medical Practice, or if it is not feasible to return or destroy Protected Health Information, protections are extended to such information, in accordance with the termination provisions of subparagraph (c) of this Section 6.

(b) *Termination for Cause*.

(1) Upon Medical Practice's knowledge of a material breach by Billing Company, Medical Practice shall provide an opportunity for Billing Company to cure the breach or end the violation and Medical Practice may terminate the Service Agreement if Billing Company does not cure the breach or end the violation within the time specified by Medical Practice;

(2) Notwithstanding the foregoing Section (b) (1), Medical Practice may immediately terminate the Service Agreement if Billing Company has breached a material term of this Agreement and Medical Practice determines that cure is not possible.

(3) Notwithstanding the foregoing Section (b) (1) or (2), if Medical Practice determines that neither cure, as specified in Section (b) (1) above nor termination, as specified in Section (b) (2) above, is feasible, Medical Practice shall report the violation to the Secretary.

(4) In the event that Billing Company becomes aware of a pattern of activity or a practice of Medical Practice that constitutes a material violation of the obligations of Medical Practice under this Agreement, Billing Company will have the same rights and obligations specified as to Medical Practice in Sections 6 (b) (1), (2) and (3).

(c) *Effect of Termination*.

(1) Except as provided in paragraph (2) of this section, upon termination of the Agreement, for any reason, Billing Company shall return or destroy all Protected Health Information received from Medical Practice or created or received by Billing Company on behalf of Medical Practice. This provision shall apply to Protected Health Information that is in the possession of subcontractors or agents of Billing Company. Billing Company shall retain no copies of the Protected Health Information.

(2) In the event that Billing Company determines that returning or destroying the Protected Health Information is not feasible, Billing Company shall provide to Medical Practice notification of the conditions that make return or destruction impossible. Billing Company shall thereafter extend the protections of this Agreement to such Protected Health Information and limit further uses and disclosures of such Protected Health Information to those purposes that make the return or destruction impossible, for so long as Billing Company maintains such Protected Health Information.

7. Miscellaneous

(a) *Regulatory References*. A reference in this Agreement to a section in the Privacy Rule, the Security Standards, or Regulations or Guidance means the referenced material as in effect as of the Effective Date or as subsequently amended or as supplemented or implemented.

(b) *State Privacy Laws.* Medical Practice will support and assist Billing Company in this regard by advising Billing Company of state privacy laws, if any, requiring non-routine confidential handling.

(c) *Amendment*. The parties agree that in the event that either party reasonably determines that the provisions of this Agreement or of the Service Agreement require amendment based on the HITECH Act (including but not limited to Guidance or Regulations to be published by the Secretary after the Effective Date of this Agreement) or other legislative or regulatory changes to the Privacy Rule or the Security Standards, the party may notify the other in writing, including the basis for its belief in reasonable detail, and the parties will thereafter promptly meet and negotiate appropriate amendments to this Agreement necessary to assure compliance by either or both the Billing Company or the Medical Practice. If the parties are unable to agree on such changes, in writing, within ____ (___) of receipt of the notice, either party may terminate the Service Agreement, without cost or penalty unless otherwise specifically provided for in the Service Agreement, upon the earlier

of (i) the date on which the proposed amendment was requried by law or Regulation to be effective or (ii) _____ (____) days advance written notice.

(d) *Survival*. The respective rights and obligations of the parties under this Agreement which required or contemplate compliance after termination of this Agreement shall survive the termination.

(e) *Interpretation*. Any ambiguity in this Agreement shall be resolved in favor of a meaning that permits both Medical Practice and Billing Company to comply with the Privacy Rule or the Security Standards, as appropriate, consistent with the Service Agreement.

In witness whereof, Medical Practice and Billing Company have executed this Business Associate Agreement, effective as set forth above.

Medical Practice	Billing Company
By: _____	By: _____
Its: _____	Its: _____